Kroll Ontrack

Sichere und endgültige Datenlöschung

von: Axel Kunz
Sales Manager, Leiter Business Development und Leiter Vertrieb Software,

Kroll Ontrack GmbH, Böblingen

Inhalt

1. Einleitung

Die Sicherheit digitaler Daten ist heute ein Thema von größter Aktualität, das noch mehr Bedeutung erhält, wenn es um die **Sicherheit personenbezogener Daten** geht. Im Zuge der Datenschutzdebatte setzen sich Gesetzgeber aus der ganzen Welt mit dem Schutz personenbezogener Daten auseinander. Die Datenschutzbehörden konzentrieren sich dabei besonders auf die Unternehmen, da immer mehr Informationen über natürliche Personen anhand von IT-Instrumenten im Zuge der Geschäftsabwicklung verarbeitet und gespeichert werden. Die Möglichkeit unerwünschter Zugriffen und die daraus folgende nicht autorisierte Entwendung, Verwendung oder Verbreitung personenbezogener Daten lässt sich nur unter der Bedingung ausschließen, dass man den auf Computern oder anderen elektronischen Geräten gespeicherten Informationen einen angemessenen Level an Schutz gewährleistet.

Der Großteil der Unternehmen investiert in Sicherheit, jedoch konzentriert sich hierbei die gesamte Anstrengung auf den Schutz der IT-Systeme in der Zeit ihrer Verwendung. Angesichts der neuen Risiken für das Persönlichkeitsrecht der Menschen ist heute allerdings etwas mehr als das erforderlich.

Wie kann man Daten schützen, auch wenn die IT-Infrastrukturen, in denen sie enthalten sind, ausrangiert, entsorgt oder wiederverwendet werden? Das ist die neue Frage, die sich Unternehmen stellt. Und dieses Problem verdient besondere Aufmerksamkeit, da aufgrund der schnellen technologischen Entwicklung der Austausch von IT-Geräten inzwischen in jeder Organisation regelmäßig erfolgt und ein Management des End-of-Life von Geräten und Medien erforderlich wird.

Die Lösung ist relativ einfach und bedeutet sicheres und endgültiges Löschen. Mit spezifischen Instrumenten ist es möglich, personenbezogene Daten nicht nur zu schützen, sondern sie auch unwiederbringlich von Computern und anderen elektronischen Geräten zu löschen, wenn Leasingverträge auslaufen, der Lebenszyklus der Hardware abgeschlossen ist oder immer dann, wenn sich das Unternehmen für die Wiederverwertung oder Ausrangierung ihrer IT-Assets entscheidet.

Wie wir auf den nächsten Seiten sehen werden, ist das sichere Löschen auch ein Bestandteil des rechtlichen Rahmens zum Datenschutz und der gesetzlichen Regelungen zum Schutz personenbezogener Daten. Das sichere Löschen ist außerdem ein wichtiger Teil der neuen General Data Protection Regulation (GDPR), deren Verabschiedung die Europäische Kommission in Kürze beabsichtigt, um den Schutz der personenbezogenen Daten innerhalb der Mitgliedsstaaten der Europäischen Union anzugleichen.

In diesem E-Book findet der Leser einen Überblick über die operativen und normativen Hauptaspekte in Bezug auf das sichere Löschen sowie den Startpunkt für einen informativen Weg, der ihn durch die folgenden vertiefenden Artikel leiten wird. Am Ende des Textes gibt es als praktisches Hilfsmittel ein nützliches Glossar mit den im Bereich des Datenschutzes am häufigsten auftauchenden Begriffen.

Peter Böhret
Managing Director
Kroll Ontrack GmbH

2. Datenschutz, die wahre Herausforderung unserer Zeit

Der Schutz elektronischer Informationen und der Datenschutz stellen für alle Unternehmen die Herausforderung unserer Zeit dar, die durch die digitale Technologie noch komplizierter wird.

Für Management und IT-Abteilungen bedeutet dies, einerseits auf Entscheidungsebene und für andererseits in der Umsetzung, eine zusätzliche Anstrengung, die in Richtung des Schutzes von IT-Systemen gehen muss, wenn diese das Ende des Lebenszyklus in der Organisation erreicht haben und als Altgeräte eingestuft werden.

Heute sind Daten, und nicht nur die personenbezogenen, gefährdeter als früher. Sie stellen einen unantastbaren Wert dar, der zunehmend kriminelle Interessen weckt. Immer häufiger erreichen uns Nachrichten über digitale Angriffe und Diebstähle digitaler Informationen. Carbanak, Sony Pictures Entertainment sowie die Online-Gaming-Plattformen von Sony Playstation und Microsoft Xbox sind nur einige Beispiele. Für jedes Unternehmen muss daher der Datenschutz und insbesondere der Schutz personenbezogener Daten nicht nur eine gesetzliche Verpflichtung darstellen sondern vielmehr eine Aufgabe zum Schutz des eigenen Unternehmens sowie der eigenen Mitarbeiter, Kunden und Lieferanten.

Gartner, Marktführer in strategischer Beratung, Forschung und Analyse im IT-Bereich hat das Thema der Sicherheit und des Datenschutzes unter den **Top 10 der technologischen Trends 2015** platziert. Es besteht kein Zweifel, dass die Verbreitung von Datenträgern die Verwaltung und Kontrolle von Informationen noch komplizierter gemacht hat. Aber genau aus diesem Grund wird heute von mehreren Seiten eine größere Aufmerksamkeit und Sensibilität für dieses Thema gefordert.

Auch die EU hat sich diesbezüglich bewegt, um den Datenschutz den neuen Gegebenheiten anzupassen. Die europäische Datenschutzrichtlinie wird durch die Verabschiedung der neuen European **General Data Protection Regulation (GDPR)** (**deutsch: EU-DSGVO/ Datenschutzgrundverordnung**) modernisiert. Die Europäische Kommission erklärt hierbei „personal data as any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address.“ („Als personenbezogene Daten gelten sämtliche Informationen, die eine natürliche Person betreffen, unabhängig davon, ob diese in Zusammenhang mit ihrem privaten, beruflichen oder öffentlichen Leben stehen. Dabei kann es sich um alles Mögliche handeln, von einem Namen, einer Fotografie, einer E-Mail-Adresse, Bankdaten, Posts in sozialen Netzwerken, medizinischen Informationen bis zur IP-Adresse des Computer.“)

Die GDPR vereint alle Gesetze zum Schutz personenbezogener Daten, um auf die Herausforderungen des digitalen Zeitalters zu reagieren und besonders, um den Online-Schutz zu verstärken. Neben weiteren Schutzmaßnahmen wird die Verordnung durch ihre Einführung alle Unternehmen, die personenbezogene Daten von Menschen in der EU verwalten, verpflichten, diese Informationen zu löschen, wenn dies angefordert wird oder sie für die Organisation nicht mehr notwendig sind.

Die Auflagen zum Datenschutz werden immer weiter verstärkt werden und dieser Trend wird sich auch in der Zukunft immer weiter fortsetzen. Den Unternehmen wird empfohlen, sofort damit zu beginnen, ihre Situation intern oder mit Hilfe von Experten zu bewerten, um eventuelle Mängel zu beseitigen.

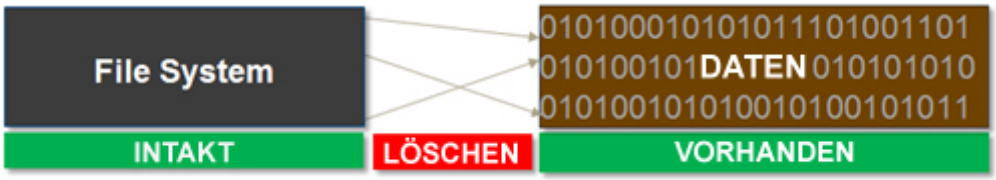
3. Was ist sicheres Löschen von Daten?

Wie bereits am Anfang dieses E-Books erwähnt wurde, stellen das Ausrangieren, die Entsorgung und die Wiederverwertung von IT-Assets einen Moment der größten Verwundbarkeit für die Daten dar. Firmen, die einzelne PCs, mobile Geräte oder Serversysteme ausrangieren, tun dies häufig ohne besondere Vorsichtsmaßnahmen.

Im besten Fall sorgen die IT-Abteilungen durch Eingabe eines vom Betriebssystem zur Verfügung gestellten Löschbefehls für eine oberflächliche Löschung der Inhalte. Im ersten Fall bleiben die personenbezogenen Daten ebenso wie alle weiteren Informationen komplett sichtbar und für jeden zugänglich, der Zugriff auf die betreffende Hardware hat (Altgeräte werden häufig zu wohltätigen Zwecken gespendet oder gebraucht verkauft). Im zweiten Fall reicht eine **einfache Wiederherstellungssoftware**, um die vermeintlich gelöschten Dateien problemlos wiederherzustellen.

Es ist eine weit verbreitete Meinung, dass der Befehl Löschen, das Leeren des Papierkorbs oder die Formatierung eines Laufwerks geeignete Lösungen zum schnellen und endgültigen Löschen sämtlicher Spuren einer Datei seien. Viele IT-Abteilungen glauben, auf diese Weise aus technischer Sicht das Dilemma zu lösen, wie man Datenträger ausrangiert, ohne dass die vorher auf ihnen gespeicherten Daten wiederherstellbar sind. Leider bedeutet die Tatsache, dass die Inhalte nicht mehr sichtbar sind, jedoch nicht, dass sie nicht mehr auf dem Gerät vorhanden sind. Diese Art des Löschens, die man als einfaches Löschen definieren könnte, führt nämlich lediglich zur Vernichtung der Zeiger, die dem Betriebssystem anzeigen, wo sich die Dateien befinden. **Sie führt jedoch nicht zur definitiven Vernichtung des Inhalts der Dateien selbst.**

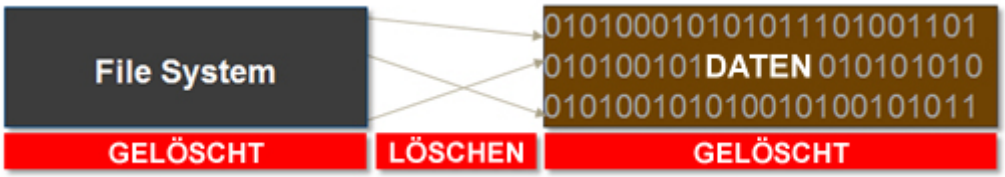
Schaubild 1 – Einfache Datenlöschung löscht nur das Verzeichnis, nicht die Daten selbst



Stellen wir uns ein Buch vor. Am Anfang findet man ein Inhaltsverzeichnis, das die Position der Kapitel anhand der Seitenzahlen angibt. Das einfache Löschen eines Geräts entspricht dem Vernichten des Inhaltsverzeichnisses eines Buchs: man weiß zwar nun nicht mehr, an welcher Stelle sich ein bestimmtes Kapitel befindet, aber wenn man das Buch durchblättert, wird man keine Schwierigkeiten haben, es wiederzufinden.

Anders als das einfache Löschen **wirkt das sichere Löschen sowohl auf die Zeiger als auch auf den Inhalt der Dateien selbst**: tatsächlich lässt sich so nichts wiederherstellen, da nichts von der Originalinformation auf dem Gerät zurückbleibt. Um bei dem Beispiel des Buches zu bleiben, hätten wir uns in diesem Fall also entschieden, neben dem Inhaltsverzeichnis auch alle Seiten der Kapitel zu vernichten.

Schaubild 2 – Die sichere Datenlöschung löscht das Verzeichnis sowie die Daten selbst



Das *Überschreiben*, über das wir eingehender in Absatz 6 sprechen werden, ist eine technische Maßnahme zum sicheren Löschen von Daten, die nicht nur die Zeiger, sondern auch die Dateien selbst vernichtet. Die auf sichere Weise gelöschten Daten sind **nicht mehr auf dem Datenträger vorhanden**, weshalb es folglich **unmöglich ist, sie zu rekonstruieren**. Dies gilt nicht nur für die Verwendung entsprechender Software, sondern auch Datenrettung-Spezialisten.

Nun ist es wohl verständlicher, warum das sichere Löschen auch die einzige Form des Löschens ist, die zur Protektion der von den Datenschutzgesetzen geschützten personenbezogenen Daten angewendet werden kann.

4. Zwischen gesetzlicher Verpflichtung und firmentechnischer Notwendigkeit

Die definitive Vernichtung von Daten ist keine Möglichkeit, die dem einzelnen Unternehmen überlassen bleibt. Dennoch - mehr als nur eine gesetzliche Verpflichtung - sollte man das sichere Löschen als eine Best-Practice zum Schutz der firmeneigenen Daten betrachten, unabhängig von ihrer Art. Der Schutz der personenbezogenen Daten von Kunden, Lieferanten und Angestellten ist schließlich eine Regel des gesunden Menschenverstands.

Ebenso verhält es sich mit dem Schutz vertraulicher und geheimer Geschäftsdaten, wie zum Beispiel solchen, die unter das Recht des geistigen Eigentums fallen, ebenso wie Entwicklungsprojekte neuer Produkte, Rechnungsunterlagen oder E-Mail-Verkehr. Gemäß den Daten des Forschungsinstituts Eurispes zu IT und Sicherheit wurde 2013 in Deutschland mindestens eine Milliarde Euro für Lösungen im Bereich der IT-Sicherheit ausgegeben.

Es ist jedoch offensichtlich, dass alle Investitionen in den Schutz von IT-Systemen und Informationen zunichte gemacht werden, wenn man das Sicherheitskonzept ausgerechnet in dem Moment vernachlässigt, in dem die Hardware ausrangiert wird und die Daten noch verwundbarer sind.

Der Schutz personenbezogener Daten und digitaler Informationen bedeutet also keine Erschwerung der IT-Vorgänge, sondern ist eine Investition in die Sicherheit, die dem Wohlstand der Firma nützt und diejenigen schützt, die mit ihr interagieren. Um den sogenannten Qualitätssprung zu vollführen, ist es insbesondere notwendig, sich die Sicherheit als einen Prozess und nicht als ein Produkt vorzustellen. Sicherheit ist nämlich zuallererst ein kultureller Ansatz: man benötigt ein größeres Bewusstsein über die Probleme, die durch den unkorrekten Umgang mit Daten verursacht werden, ebenso wie Kenntnisse über die angemessene Verwendung der IT-Instrumente, die ein unabdingbares Mittel zum Erreichen der Ziele darstellen.

Konkret bedeutet das: Damit das sichere Löschen zur Firmenkultur wird, darf es nicht dem guten Willen einzelner User und ebenso wenig der Initiative der IT-Abteilungen überlassen bleiben. Das sichere Löschen muss in den Firmenalltag als eine Richtlinie unter den Angestellten eingeführt werden, damit diese ein

klares Bewusstsein dazu entwickeln. Als logische Konsequenz muss die IT mit angemessenen Instrumenten ausgestattet werden, um diese Richtlinie korrekt umsetzen zu können. Wie in den folgenden Absätzen zu lesen sein wird, ist es nicht einmal notwendig, dass der Löschprozess direkt vom IT-Mitarbeiter der Firma durchgeführt wird. Dies vereinfacht die Umsetzung der Verpflichtung noch weiter, da man die Aufgabe somit an externe Dritte übertragen kann

5. Die rechtlichen Rahmenbedingungen in der Bundesrepublik Deutschland

Nach den schrecklichen Erfahrungen in Deutschland während der nationalsozialistischen Diktatur und seiner massiven Eingriffe in die persönlichen Rechte eines jeden einzelnen Bürgers wurde im Grundgesetz der Bundesrepublik Deutschland in Artikel 1 Absatz 1 das allgemeine Persönlichkeitsrecht verankert. Nach dem Urteil des Bundesverfassungsgerichtes in der Auseinandersetzung um die Volkszählung gehören dazu auch die persönlichen Daten eines jeden Bürgers.

Allerdings wurde der Bereich des Datenschutzes nicht gleich nach dem Krieg, sondern erst relativ spät gesetzlich auf Bundesebene geregelt und zwar 1977 mit der ersten Fassung des Bundesdatenschutzgesetzes. Zuvor wurden Schutzrechte für persönliche Informationen und Daten von Bürgern innerhalb verschiedener Gesetze gewährleistet wie z.B. das Postgeheimnis, das Steuergeheimnis, das Beichtgeheimnis oder die ärztliche Schweigepflicht in den jeweiligen Gesetzen bzw. Verordnungen. Mit dem Beitritt der ehemaligen DDR in die Bundesrepublik wurden auch in den neugeschaffenen Bundesländern eigene Landesdatenschutzgesetze geschaffen sowie die Geltung des Bundesdatenschutzgesetzes in den neuen Bundesländern übernommen.

Der Datenschutz in Deutschland ist in einer Vielzahl von Gesetzen geregelt. Dabei kann man zwischen Datenschutzgesetzen für den öffentlichen Bereich und Datenschutzgesetzen für den privaten Bereich und der Privatwirtschaft unterscheiden. Zudem hat jedes Bundesland der Bundesrepublik ein eigenes Datenschutzgesetz, da sich die Schutzvorschriften auf Landes- und kommunaler Behörden-Ebene beziehen. Denn eine ausdrückliche Kompetenz des Bundes zur umfassenden Regelung des Datenschutzes enthält das Grundgesetz nicht.

Wenn Verwaltungstätigkeiten des Bundes oder Bundesrechte im öffentlichen Bereich betroffen sind und wenn es sich um Datensammlungen im privatwirtschaftlichen Bereich handelt, gelten generell die Paragrafen des Bundesdatenschutzgesetzes.

Daneben gibt es noch bereichsspezifische Datenschutzregelungen, die in Spezialgesetzen enthalten sind. Diese sind **vorrangig** zu berücksichtigen. Solche Spezialgesetze sind beispielsweise das Kreditwesen- und Geldwäschegesetz sowie das Telekommunikationsgesetz und die Telekommunikationsüberwachungsverordnung.

5.1 Das Bundesdatenschutzgesetz (BDSG)

Im Bundesdatenschutzgesetz (BDSG) wird der Umgang mit personenbezogenen Daten geregelt.

Der Zweck des BDSG wird bereits in § 1 Abs. 1 kurz und knapp genannt:

„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“

Personenbezogen sind Daten dann, wenn sie persönliche oder sachliche Verhältnisse einer natürlichen Person beschreiben. Dabei muss die Person nicht namentlich bekannt sein, sondern es genügt, wenn sie bestimmbar ist (wie z.B. aus der Telefonnummer, der E-Mail-Adresse, der IP-Adresse beim Internet-Surfen oder der Personalnummer). Das BDSG regelt dabei die Datenerhebung, die Datenverarbeitung und die Datennutzung. Unter Erhebung ist die Beschaffung von Daten über natürliche Personen und unter Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen der Daten zu verstehen. Während unter der Nutzung die eigentliche Verarbeitung der Daten im Rahmen der Analyse zu verstehen ist, soweit es nicht um eine der unter Verarbeitung genannten Tätigkeiten handelt.

Dabei ist das Bundesdatenschutzgesetz **ein Verbotsgesetz mit Erlaubnisvorbehalt**, das heißt es ist alles verboten, was nicht ausdrücklich erlaubt ist! Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist also im Prinzip verboten. Erlaubt ist sie also nur dann, wenn es eine gegenteilige Rechtsgrundlage gibt (d.h. ein Gesetz erlaubt die Datensammlung in diesem Fall) oder die betroffene Person stimmt ihr (meist schriftlich) explizit zu (§ 4, Absatz 1, § 4a). Zudem gilt der in § 3a definierte Grundsatz der Datensparsamkeit und Datenvermeidung mit dem Ziel, so wenig wie möglich personenbezogene Daten zu erheben und bei einer Datenerfassung möglichst von einer Anonymisierung oder Para-Anonymisierung Gebrauch zu machen.

Zusammenfassend betrachtet ist eine Datensammlung also dann erlaubt, wenn

- eine persönliche Erlaubnis des Betroffenen vor der Verarbeitung vorliegt oder
- ein Gesetz oder eine Rechtsvorschrift dazu vorliegt.

Laut Bundesdatenschutzgesetz hat der betroffene Bürger gegenüber allen speichernden Stellen das Recht auf

- Auskunft
- Berichtigung
- Löschung
- Sperrung

Zudem besteht ein Recht auf

- Unaufgeforderte Benachrichtigung
- Schadensersatz
- Einsicht in das Datenregister der Kontrollbehörden
- Anrufung des Datenschutzbeauftragten

Die Aufsicht über den Datenschutz wird durch die jeweiligen Datenschutzbeauftragten der Bundesländer durchgeführt. Das bedeutet in der Praxis, dass bei einem Verstoß der zuständige Landesbeauftragte für den Datenschutz und die Informationsfreiheit des jeweiligen Bundeslandes angerufen werden muss. Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit kontrolliert hingegen vorrangig die jeweiligen Aufsichtsbehörden der Bundesländer.

Das Bundesdatenschutzgesetz wurde im Laufe der Jahre mehrmals erweitert oder geändert. Hintergrund ist sowohl die Einhaltung nationaler als auch europäischer Datenschutzrichtlinien, die in das deutsche Recht integriert werden mussten, bevor sie hierzulande rechtsgültig sind.

5.2 Strafen bei Nichtbeachtung der Paragrafen des BDSG

Datenschutzvergehen sind keine Kavaliersdelikte. Ganz im Gegenteil. Deshalb hat der Gesetzgeber zum Teil drastische Strafen bei Missachtung der in diesem Gesetz formulierten Vorschriften erlassen. Dabei wird unterschieden zwischen Ordnungswidrigkeiten und Strafvorschriften. Die Ordnungswidrigkeiten umfassen insgesamt 18 Punkte – unter anderem, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind abruft, erhebt oder verarbeitet – und können je nach Schwere des Vergehens mit einer Geldbuße von entweder 50.000 oder bis zu 300.000 Euro geahndet werden. Dazu steht in § 43: „Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden".

Richtig teuer wird es für ein Unternehmen dann, wenn es gegen § 44 des BDSG verstoßen hat. Wer beispielsweise unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind abruft, erhebt oder verarbeitet „gegen **Entgeld** oder in der **Absicht, sich oder einen anderen zu bereichern** oder einen anderen **zu schädigen**,…, wird mit **Freiheitsstrafe bis zu zwei Jahren** oder mit Geldstrafe bestraft."

Allerdings wird die Tat nur auf Antrag durch den Betroffenen, der Aufsichtsbehörde oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verfolgt.

5.3 Was ändert sich mit der europäischen Datenschutzgrundverordnung (EU-DSGV)?

Wie bereits an anderer Stelle ausgeführt, müssen europäische Rechtsnormen normalerweise in die deutsche Gesetzgebung übernommen werden, bevor sie auch hier Gesetzeskraft haben. Bei der europäischen Datenschutzgrundverordnung ist das anders: **Sie gilt unmittelbar nach Inkrafttreten Anfang 2018! Es bedarf keiner Umsetzung mehr in deutsches Recht.**

Aufgrund der im Vertrag vereinbarten Öffnungsklauseln ist aber davon auszugehen, dass selbst wenn das BDSG noch nicht aufgehoben sein sollte und die Regelungen des EU-DGSV unmittelbaren Anwendungsvorrang genießen, das BDSG soweit überarbeitet wird, dass es einen widerspruchsfreien Übergang geben wird.

Dabei ist es unerheblich, ob die kommenden Datenschutzbestimmungen der am 14. April 2016 nach vierjähriger Beratung vom europäischen Parlament beschlossenen neuen europäischen Datenschutzgrundverordnung (EU-DSGVO oder auch GDPR genannt) in das BDSG übernommen oder über mehrere Gesetze verteilt werden. Man kann allerdings davon ausgehen, dass die wichtigsten Änderungen bzw. Verschärfungen des EU-DSGV bis 2018 in ein geändertes BDSG einfließen werden.

Tatsache ist, dass die in der EU-DSGVO getroffenen Paragrafen, auf eine Angleichung der Datenschutzgesetze in allen europäischen Staaten ausgelegt sind. Das bedeutet für Unternehmen, unabhängig von ihrem Hauptsitz, dass beim Handel in der Europäischen Union die Bestimmungen des EU-DSGVO einzuhalten sind. Die Bestimmungen der EU-DSGVO werden in fast allen europäischen Mitgliedsländern in die nationalen Gesetze einfließen.

Die europäische Datenschutzgrundverordnung wird also im Frühjahr 2018 auf jeden Fall in Kraft treten und damit auch die Rechtsnormen. Das Stufensystem der neuen Gesetzgebung sieht **dabei bereits Strafen von bis zu zwei Prozent des weltweit erwirtschafteten Jahresumsatzes vor, wenn Verarbeitungsvorgänge nicht ordnungsgemäß dokumentiert würden (Artikel 28).** Bei einer Verletzung der Datensicherheit seien Unternehmen verpflichtet, innerhalb von 72 Stunden die Behörden zu informieren (Artikel 31).

Im Vergleich zum BDSG wurden im Wesentlichen die gleichen Vergehen beim Datenschutz auch hier in Gesetzesform gegossen. Genauso wie im bereits geltenden deutschen Datenschutzgesetz handelt es sich auch hier um ein Verbotsgesetz mit Erlaubnisvorbehalt. Auch die Vorgabe der „Datensparsamkeit“ und der Anonymisierung, die bereits in das BDGS Eingang gefunden hatte, ist auch in der EU-Verordnung integriert. Änderungen bzw. Ergänzungen finden sich besonders in zwei Feldern:

1. Die Datenrichtigkeit

„Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)”. (Art .5 Abs. 1d DSGVO)

*Bislang wurden die **berechtigten Berichtigungs- und Löschansprüche** der Betroffenen mit § 35 des BDGS begründet. Bereits in diesem Gesetz sind unrichtige, unzulässig gespeicherte, nicht mehr benötigte und weitere geschäftsmäßig genutzte Daten zu löschen oder – nach Ende eines Vertrages – wenn der Betroffene dies verlangt.*

Im neuen EU-DSGVO wird das ganze nochmals verschärft! Wie oben zu lesen ist, muss jetzt der Datensammler zusätzlich darauf achten, dass die Daten während der gesamten Laufzeit korrekt sind.

2. Verantwortlichkeit/Dokumentation

Neu ist die – ausdrückliche – Regelung, dass über die Einhaltung der datenschutzrechtlichen Grundsätze **Rechenschaft** abzulegen ist („Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“). Das bedeutet, dass Unternehmen in ein dokumentiertes Datenschutzkonzept investieren sollten, um Haftungsrisiken abzusichern.

Wie auch bereits im Bundesdatenschutzgesetz ausgeführt, enthält auch das neue EU-DSGVO die Speicherungsfristen der gesammelten Daten. Fristen haben sich unverändert an der Erforderlichkeit für den Verarbeitungszweck zu orientieren:

„Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; […] (“Speicherbegrenzung”)”. (Art. 5 Abs.1 e) DSGVO)”.

Das bedeutet, dass auch weiterhin und (wahrscheinlich noch viel wichtiger als zuvor) praktikable Löschkonzepte in den Unternehmen etabliert sein oder werden müssen. Denn was sich geändert hat, sind die …

5.4 Strafen bei Nichtbeachtung des EU-DSGVO/GDPR

Insgesamt wurden die Strafen für fahrlässigen oder absichtlich schlechten Datenschutz im Vergleich zu den Strafzahlungen im Bundesdatenschutzgesetz empfindlich verschärft. So sieht der neue europäische Datenschutz bei Verstößen massive Bußgelder **von bis zu 20 Million Euro oder vier Prozent des jeweiligen Jahresumsatzes vor**.

6. Technische Maßnahmen zum sicheren Löschen

Die **technischen Maßnahmen** zum sicheren Löschen der Daten, die auf elektronische oder IT-Geräte angewendet werden können, werden in der folgenden Tabelle aufgeführt:

Sollen die Geräte **wiederverwendet** oder **recycelt** werden, wird ein effektives Löschen der Daten folgendermaßen erreicht:	Sicheres Löschen *optischer* oder *magnetisch-optischer* Datenträger, die für die **Entsorgung** bestimmt sind, kann auch durch folgende Prozeduren erfolgen:
• Software-Überschreibung (*wiping program*) • Formatierung auf niedriger Stufe (*low level formatting*) • Entmagnetisierung magnetischer Geräte (*degaussing*)	• Schreddern oder mechanische Deformierung • Physikalische Zerstörung oder Auflösung • Entmagnetisierung auf hoher Stufe

Schauen wir uns zusammenfassend jede dieser Möglichkeiten an.

6.1 Software-Überschreibung

Wie der Begriff vermuten lässt, schreibt eine Software zum Überschreiben *„… zufällige Sequenzen ‚binärer' Ziffern (Null und Eins)…"* über die vormals auf dem Medium existierenden Daten. Um größere Sicherheit zu gewährleisten und das Risiko einer Rekonstruktion der Originalinformationen mit einer Datenrettungs-Software oder technischen Eingriffen zur Datenwiederherstellung weitestgehend unmöglich zu machen, wird der Vorgang des Überschreibens mehrfach wiederholt.

Auch wenn ein einziges Überschreiben (technisch *Erasing*) ausreichende Garantien für die definitive Vernichtung der Daten geben kann, empfiehlt die Datenschutzbehörde, dass *„die Anzahl der Wiederholungen des Vorgangs eine angemessene Sicherheit erreicht (die sich je nach Vertraulichkeit oder Wichtigkeit der Daten zu richten hat, deren unrechtmäßige Aneignung man zu verhindern sucht), wenn zwischen sieben und fünfunddreißig Überschreibungen vorgenommen werden…".*

Die Anzahl der Erasings hat einen Einfluss auf die für das Löschen verwendete Zeit, die von einigen Stunden bis zu einigen Tagen dauern kann. Auch die Schreibgeschwindigkeit des Datenträgers, der überschrieben werden soll, spielt hierbei eine Rolle.

6.2 Formatierung auf niedriger Stufe

Eine besondere Art der Formatierung, die auf Festplatten angewendet werden kann. Hierbei muss man den Anweisungen folgen und eventuelle vom Hersteller zur Verfügung gestellte Software verwenden.

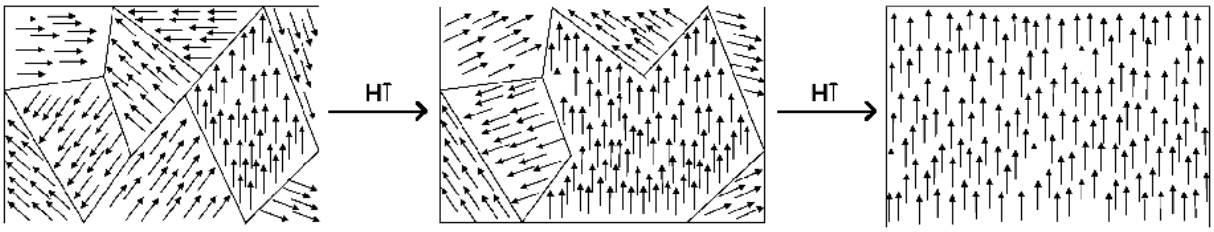
6.3 Entmagnetisierung

Eine besondere Technik zum definitiven Löschen von Daten, die auf *magnetische* oder *magnetisch-optische* Speichermedien angewendet werden kann (Festplatten, Disketten, Magnetbänder auf offenen Spulen oder in Kassetten). Die Entmagnetisierung gewährleistet ein schnelles Löschen der Informationen auch von kaputten Datenträgern, bei denen die Software-Überschreibung nicht angewendet werden kann.

Das zugrunde liegende physikalische Prinzip der Entmagnetisierung beruht auf der **Weiss'schen Polarisierung der Domänen**.

Die Daten werden auf magnetischen Datenträgern, wie Festplatten oder Magnetbänder, gespeichert, wobei ein Magnetfeld mit sehr kleinen Teilchen, die **magnetische Domänen** oder nach dem französischen Physiker Pierre-Ernest Weiss, der diese Theorie entwickelte, **Weiss-Bezirke** genannt werden. In der Phase des Beschreibens mit Informationen richtet sich das Magnetfeld in eine bestimmte Richtung aus, beziehungsweise orientiert die Magnetisierung einer bestimmten Anzahl Weiss-Bezirke. Den Richtungen der Magnetisierung sind die Bit-Werte 0 und 1 zugeordnet.

Schaubild 3 – Vergrößerung der Weiss-Bezirke durch die Ausrichtung mehrerer Domänen über ein externes magnetisches Feld



Wenn man nun einen magnetischen Datenträger dem Degaussing unterzieht, wird die Magnetisierung der Weiss-Bezirke verändert, so dass sie nicht mehr in eine einheitliche Richtung sondern zufällig ausgerichtet sind. Als Folge hiervon sind die Daten nicht mehr zugänglich oder rekonstruierbar.

Für die Entmagnetisierung wird ein Hardware-Apparat namens *Degausser* in der entsprechenden Stärke benötigt. Anders als bei Software-Programmen zum Überschreiben, beträgt die für die Fertigstellung einer Degaussing-Löschung aufgewendete Zeit nur wenige Sekunden.

Ein zweiter Unterschied zur Software-Überschreibung besteht darin, dass ein entmagnetisierter Datenträger in der Regel nicht wiederverwendet werden kann.

6.4 Ausstanzung oder mechanische Deformierung

Unter Ausstanzung versteht man eine Durchlöcherung, die durch Pressen oder Schlagen mit einer Punze in die zu durchlöchernde Oberfläche erzielt wird. Die mechanische Deformierung hingegen wird durch die Deformierung des Datenträgers erreicht, also durch die Veränderung seiner Geometrie, Größe oder Form.

6.5 Physikalische Zerstörung oder Schreddern

Hierbei handelt es sich um die Zerkleinerung des Datenträgers mit hierfür vorgesehenen Apparaten, die über entsprechende Schneidewerkzeuge verfügen. Die Datenschutzbehörde behält diese Lösung dem Umgang mit optischen Datenträgern wie, CD-Roms und DVDs, vor.

6.6 Entmagnetisierung auf hoher Stufe

Anwendbar auf magnetische Datenträger, wie bereits unter Punkt *6.3 Entmagnetisierung* aufgeführt, und auch auf kaputte Geräte, bei denen die Software-Überschreibung nicht angewendet werden kann.

7. Welche Geräte müssen gelöscht werden

Nicht nur auf Computern (*Desktops*, *Laptops* oder *Servern*) sollte das sichere Löschen angewendet werden, sondern auch auf *bewegliche* oder *abnehmbare* Datenträger.

Tatsächlich gibt es keine vorgefertigte Liste der Datenträger, auf die notwendigerweise das sichere Löschen angewendet werden muss: weder das Gesetzbuch noch die Durchführungsmaßnahme der Datenschutzbehörde nehmen Bezug auf eine vorgefertigte Liste der Speichermedien. Die Gesetzgebung spricht im Allgemeinen von ***elektronischen Datenträgern*** und die gesetzliche Verpflichtung bezieht sich auf die Art der darauf enthaltenen Daten.

Jedwede Art von Speichermedium, auf dem sich personenbezogene Daten befinden, müssen sicher gelöscht werden. Und wie wir gesehen haben, sollte dies auch für jeden Datenträger mit Informationen, die geheim oder vertraulich behandelt werden sollen, gelten.

Festplatten, SSDs, Flash-Speicher verschiedener Art und Formats, USB-Sticks und Magnetbänder sind nur eine kleine Sammlung der in Frage kommenden Datenträger. Eine relativ neue, aber besonders kritische Storage-Kategorie besteht in den **mobilen Datenträgern**.

Smartphones und *Tablets* bieten – trotz ihrer reduzierten Größe – heute einen beachtlichen Speicherplatz und gehören inzwischen zur Standardausstattung der meisten Angestellten von Unternehmen jeder Art. Smartphones stellen hierbei mit 91% Anwendung in Firmen das am weitesten verbreitete Instrument dar, gefolgt von Tablets mit 66% Verbreitung.

Es ist also sehr wichtig, in Firmen ausrangierte bewegliche Datenträger, den Prozeduren des sicheren Löschens zu unterziehen. Man muss bedenken, dass sich auf *Smartphone* und *Tablets* die gleichen Informationen befinden, die man auch auf Geräten wie Desktops oder Laptops finden kann (z.B. E-Mails und Dokumente). Es sind sogar noch mehr, wenn wir einmal an SMS, Telefonbuch und Anrufregister denken. Die Angelegenheit wird in den Firmen noch deutlich komplizierter, die **BYOD** (*Bring Your Own Device*) anwenden, in denen also der Angestellte sein persönliches Gerät auch für die Arbeit benutzt. Da hier nicht mehr zwischen privaten und beruflichen Daten unterschieden werden kann, würden beim sicheren Löschen auch all die Informationen vernichtet werden, die dem privaten Gebrauchs des Gerätebesitzers entstammen.

Es ist also sachdienlich, wenn Unternehmen auch dies aufmerksam in Erwägung ziehen, bevor sie sich für eine Umsetzung von BYOD im eigenen Betrieb entscheiden.

8. Professionelle Instrumente zum sicheren Löschen von Daten

Die Wahl der Software- oder Hardware-Lösungen, mit denen das sichere Löschen in der eigenen Firma umgesetzt werden soll, verdient große Aufmerksamkeit. Nicht alle auf dem Markt erhältlichen Software- oder Hardware-Lösungen verfügen über die gleiche Wirksamkeit und vor allem über geeignete Eigenschaften, um dem Unternehmen die Konformität mit der Datenschutzgesetzgebung zu gewährleisten. Weiterhin sollte man Do-it-yourself-Lösungen meiden, da diese in Bezug auf die Wirksamkeit sehr risikoreich und absolut ungeeignet sind, um der Firma ein professionelles und verifizierbares sicheres Löschen anzubieten.

Mit den richtigen Instrumenten hingegen ist es möglich, einen **gesetzeskonformen,** einfach zu handhabenden und kostengünstigen Prozess für das einzelne zu löschende Gerät umzusetzen. Professionelle Produkte zeichnen sich durch folgende Eigenschaften aus:

- *Unabhängige Zertifizierungen*
- *Verwendung internationaler Standard-Algorithmen*
- *Zweckdienliche technische Eigenschaften*
- *Detaillierte Berichterstattung*
- *Verfolgbarkeit der ausgeführten Löschvorgänge*

Sie garantieren dem Unternehmen die volle *Compliance* der Gesetze und Vorschriften. Die Lösungen von Kroll Ontrack erfüllen jedes Bedürfnis auf dem Gebiet des sicheren Löschens und beinhalten:

- Software-Überschreibung
- Hardware zum Entmagnetisieren
- Serviceleistungen von spezialisierten Technikern

8.1 Datenlösch-Software

Kroll Ontrack ist Premium-Reseller der Software-Produkte von Blancco, dem Marktführer im Bereich des sicheren Löschens von Daten, entwickelt jedoch auch eigene Serviceleistungen und Lösungen. Das Blancco-Software-Sortiment umfasst Produkte, die spezifisch für den zu löschenden Datenträger entwickelt wurden.

Für jeden Datenträger kann also die seinen Eigenschaften am besten entsprechende Software angewendet werden:

- **Blancco 5 PC** – Löscht Festplattenlaufwerke und Solid State Drives von Computern, Desktops und Laptops
- **Blancco 5 Server** – Vernichtet die Daten von Servern
- **Blancco 5 Mobile** – Für mobile Datenträger, wie Smartphones und Tablets
- **Blancco Flash** – Entwickelt für die Anwendung auf Speicherkarten, USB-Sticks und andere Flash-Speichergeräte
- **Blancco File** – Selektives Löschen von Dateien und Ordnern
- **Blancco LUN** – Spezifisch für logische Laufwerke (*Logic Unit Number*)

Das prestigeträchtige *NATO Information Assurance Technical Centre* nahm den **Ontrack Earaser Degausser** in den ***NATO Information Assurance Product Catalogue***[1] auf*:*

- **Detaillierte Berichterstattung** über jeden Löschvorgang, unabdingbar zum Beleg für die Durchführung der Tätigkeit
- Wahlmöglichkeit zwischen **verschiedenen Algorithmen zum sicheren Löschen**, internationale Standards
- **Zahlreiche Zertifizierungen und Empfehlungen** unabhängiger dritter Stellen

Der einfache Umgang mit dieser Produktplattform wird von einer *Web-Konsole* als Hosting oder Eigentum gewährleistet, über welche man die **Verwaltung der Lizenzen und der Löschberichte zentralisieren** kann. Die Firma kann so an einem einzigen Ort sämtliche Löschprozesse ihrer IT-Assets visualisieren und verfolgen.

8.2 Entmagnetisierungs-Hardware

Ontrack Eraser Degausser ist die professionelle Hardware zum sicheren Löschen mit Entmagnetisierung (*degaussing*). Dieser Degausser ist das stärkste auf dem Markt erhältliche Gerät und kann ein Magnetfeld von bis zu 18.000 Gauss erzeugen.

Ein Magnetfeld von dieser Kraft bietet nicht nur die Garantie, erfolgreich alle Daten von Festplatten der neuesten Generation zu vernichten, sondern es **bewahrt die Investition auch für die Zukunft**, in der mit dem Einsatz von Datenträger mit *Aufzeichnungsdichte* und noch höheren *Koerzivitätswerten* gerechnet werden kann.

Denn nicht alle Degausser sind in der Lage, Daten definitiv von Festplatten und Tapes zu vernichten. Man muss wissen, dass ein magnetischer Datenträger der **Entmagnetisierung einen gewissen Widerstand entgegensetzt,** den man als **magnetische Koerzivität** bezeichnet. Die Koerzivität bezeichnet die Intensität des umgekehrten Magnetfelds, das man benötigt, um einem Material seine Magnetisierung zu entziehen. Damit ein Degausser effizient ist, muss er ein Magnetfeld erzeugen können, das mindestens 1,5 Mal der Koerzivität des zu löschenden Geräts entspricht[2].

Hieraus ergibt sich, dass sich die Wirksamkeit und die Anwendbarkeit auch auf die Festplatten und magnetischen Datenträger der Zukunft eines Degaussers in Proportion zu seiner Kraft verstärken. Die Degaussing-Prozedur dauert nur wenige Sekunden: es genügt, auch kaputte Geräte in den vorgesehenen Bereich zu legen und die Entmagnetisierung durch das Drücken einer Taste in Gang zu setzen. Die Medien sind nach Abschluss des Vorgangs nicht mehr verwendbar.

Ontrack Eraser Degausser ist effizient und für Menschen und Gegenstände ungefährlich. Das Magnetfeld auf Niedrigfrequenz entfaltet sich ausschließlich im Wirkungsbereich und liegt weit unter den von der ICNIRP (International Commission on Non-Ionizing Radiation Protection) festgelegten Grenzwerten für die allgemeine Aussetzung des Publikums. Ontrack Eraser Degausser ist von der NSM (National Security Authority, Sicherheitsbehörde der norwegischen Regierung) zertifiziert und für das Löschen von Datenträgern mit Informationen bis zur Geheimhaltungsstufe NATO SECRET geeignet. Zudem erhielt der Apparat die Zertifizierung CESG – The National Technical Authority for Information Assurance, der unabhängigen Zertifizierungsbehörde für IT-Technologien des Vereinigten Königreichs.

Das prestigeträchtige *NATO Information Assurance Technical Centre* nahm den **Ontrack Earaser Degausser** in den ***NATO Information Assurance Product Catalogue***[3] auf***.***

8.3 Serviceleistungen

Den Firmen, die keine Software- oder Hardware-Instrumente zum sicheren Löschen erwerben möchten, sondern es bevorzugen, sich einem **qualifizierten Drittanbieter anzuvertrauen, um den gesetzlichen Verpflichtungen nachzukommen**, bietet Kroll Ontrack zwei Arten der Serviceleistung an.

8.3.1 Serviceleistung zum sicheren Löschen von Daten

Die Techniker führen die Löschoperationen mit dem Instrument Ontrack Eraser Degausser direkt im Geschäftssitz des Kunden (*on-site*) oder an den ins Labor von Kroll Ontrack gesendeten Geräten durch (*in–house*).

Die Durchführung des Löschens wird durch die Erstellung eines entsprechenden Berichts belegt, der die erfolgte Durchführung des sicheren Löschens auf den Geräten bestätigt. Die Geräte werden anschließend entsorgt.

8.3.2 Serviceleistung zur Verifizierung des Löschens (Erasure Verification Services)

Firmen, die Löschprozesse mit intern entwickelten Instrumenten durchführen, Utilitys nutzen oder für die Vernichtung ihrer elektronischen Geräte auf die Serviceleistungen von Dritten zurückgreifen, haben immer häufiger das Bedürfnis, sich zu vergewissern, dass ihre Daten effektiv von den Devices entfernt wurden.

Die Serviceleistung zur Verifizierung des Löschens von Kroll Ontrack ist eine Antwort auf diese Notwendigkeit. Die Datenträger werden in unseren Labors von unseren Technikern mit ausgeklügelten Instrumenten zur Datenrekonstruktion analysiert, um eventuell verbliebene Spuren von Userdaten auf den Geräten festzustellen. Im Fall eines negativen Ergebnisses (keine Datenspuren gefunden) erstellt Kroll Ontrack auf Wunsch des Kunden einen Bericht über die durchgeführte Verifizierung.

Sollten hingegen Datenspuren gefunden werden, wird der Kunde umgehend informiert, damit er die notwendigen Korrekturen an seinem Löschprozess durchführen kann.

9. Schlussfolgerungen

Die enorme Menge an Informationen über *natürliche Personen*, die tagtäglich durch die IT-Systeme von Firmen aller Art gespeichert und verarbeitet werden, hat die Datenschutzbehörde veranlasst, geeignete Modalitäten festzulegen, um zu gewährleisten, dass personenbezogene Daten von nicht autorisierten Zugriffen und Verbreitungen geschützt werden.

Auf Grundlage dieser Voraussetzung kann sich ein korrekter Verarbeitungsprozess digitaler Informationen – heute – nicht mehr darauf beschränken, exklusiv während der normalen Lebensdauer der Computer und anderen elektronischen Geräte für ihren Schutz zu sorgen. Er muss sich ganz im Gegenteil dahingehend ausweiten, dass er auch den Moment umfasst, an dem die Datenträger entsorgt oder für einen anderen Zweck bereitgestellt werden.

Auf europäischem Niveau wurde mit der Verabschiedung des neuen ***European General Data Protection Regulation (GDPR*** *oder auch EU-Datenschutzgrundverordnung/ EU-DSGVO)* eine Überarbeitung des Datenschutzes durchgeführt, um den Schutz personenbezogener Daten den neuen Herausforderungen des digitalen Zeitalters anzupassen und auf den neuesten Stand zu bringen.

In diesem Szenario trägt die Lösung für die deutlich gemachten Probleme den Namen des sicheren Löschens. Eine besondere Form des Löschens, die durch die Verwendung geeigneter Techniken die definitive Vernichtung der Daten von Computern und anderen elektronischen Geräten erlaubt, ohne dass eine Rekonstruktion möglich wäre.

Der einfachste Weg zur Umsetzung besteht darin, schon beim Kauf einer neuen Hardware wenige Euro beiseite zu legen, die dann bei der Ausrangierung des Geräts verwendet werden. Firmen, die diesen Prozess intern nicht durchführen können oder wollen, haben auch die Möglichkeit, ihn an qualifizierte Dritte auszulagern und ihnen diese Tätigkeit zu übertragen.

Es ist hingegen entschieden weniger überzeugend und sehr viel riskanter, das Problem einfach zu vernachlässigen.

Mangelndes Eingreifen in bekannten Situationen von nicht korrekter Datenverwaltung und ungeeigneter Entsorgung von Computern und IT-Assets, auf denen personenbezogene Daten gespeichert sind, stellt eine *schwerwiegende Bedrohung der Sicherheit firmeneigener Informationen* dar, führt zu einem *hohen Sanktionsrisiko aufgrund der Verletzung des Datenschutzgesetzes* sowie zu einem *möglichen Schaden an Image und Ansehen*.